CLAIMS

We claim:

1. A method for providing access management through use of a plurality of server machines associated with different locations, said method comprising the acts of:

(a) receiving, at a first server machine of the plurality of server machines, an access request to access secure items from a user of a first client machine at a first location;

(b) authenticating the user of the first client machine at the first location;

(c) authenticating the first client machine;

(d) determining whether the user is permitted to gain access to secure items via the first location when said authenticating (b) and (c) are successful;

(e) permitting the user to gain access to secure items via the first server machine when said determining (d) determines that the user is permitted to gain access to secure items from the first location; and

(f) preventing the user to gain access to secure items via the first server machine when said determining (e) determines that the user is not permitted to gain access to secure items from the first location.

2. A method as recited in claim 1, wherein said determining (d) comprises:

(d1) obtaining access privileges associated with the user to determine at least permitted locations for the user; and

(d2) determining whether the user is permitted to gain access to secure items from the first location based on the permitted locations associated with the user.

3. A method as recited in claim 1, wherein, when permitted by said permitting (e), the user gains access to secure items from the first location via the first client machine and the first server machine.

4. A method as recited in claim 1, wherein, when permitted by said permitting (e), the user gains access to secure items from the first location via the first client machine and the first server machine.

5. A method as recited in claim 1, wherein said method comprises the acts of:

(g) preventing the user from gaining access to secure items via any of the server machines other than the first server machine when said determining (d) determines that the user is permitted to gain access to secure items from the first location.

6. A method as recited in claim 1,

wherein said determining (d) comprises determining whether the user is permitted to gain access to secure items via the first client machine and the first server machine, and

wherein said permitting (e) operates to permit the user to gain access to secure items via the first client machine and the first server machine when said determining (d) determines that the user is permitted to gain access to secure items via both the first client machine and the first server machine.

7. A method as recited in claim 1,

wherein said determining (d) comprises determining whether the user is permitted to gain access to secure items via the first server machine, and

wherein said permitting (e) operates to permit the user to gain access to secure items via the first server machine when said determining (d)

determines that the user is permitted to gain access to secure items via the first server machine.

8. A method as recited in claim 1,

wherein said determining (d) comprises determining whether the user is permitted to gain access to secure items via the first client machine, and

wherein said permitting (e) operates to permit the user to gain access to secure items via the first client machine when said determining (d) determines that the user is permitted to gain access to secure items via the first client machine.

9. A method as recited in claim 1, wherein said method comprises the acts of:

(g) preventing the user from gaining access to secure items via any of the server machines other than the first server machine when said determining (d) determines that the user is permitted to gain access to secure items from the first location.

10. A method as recited in claim 9, wherein said preventing (g) of the user to gain access to secure items via any of the other server machines comprises reconfiguring at least any of the other server machines that previously permitted the user to gain access to secure items therethrough.

11. A method as recited in claim 10, wherein said permitting (e) of the user to gain access to secure items via the first server machine comprises reconfiguring the first server machine to permit access by the user to secured items via the first server machine.

12. A method as recited in claim 11, wherein said determining (d) comprises:

(d1) obtaining access privileges associated with the user to determine at least permitted locations for the user; and

(d2) determining whether the user is permitted to gain access to secure items from the first location based on the permitted locations associated with the user.

13. A method as recited in claim 1, wherein said permitting (e) of the user to gain access to secure items via the first server machine comprises reconfiguring the first server machine to permit access by the user to secured items via the first server machine.

14. A method as recited in claim 1, wherein each of the secure items is a secured file, the secured file having a format that comprises a header including security information as to who and how the secure item can be accessed; an encrypted data portion including data of the secure file encrypted with a file key according to a predetermined cipher scheme, and wherein the header is attached to the encrypted data portion to generate the secured file.

15. A method as recited in claim 14, wherein the security information in the header of the secured file facilitates the restricted access to the secured file.

16. A method as recited in claim 15, wherein the security information in the header of the secured file points to or includes the access rules and a file key.

17. A method as recited in claim 14, wherein the security information is encrypted with a user key associated with a user.

18. A method as recited in claim 14, wherein the security information includes the file key and access rules to the restricted access to the secured file.

19. A method as recited in claim 18, wherein the file key is retrieved to decrypt the encrypted data portion in the secured file when access privilege of the user is within access permissions by the access rules.

20. A method as recited in claim 18, wherein the access rules are expressed in a markup language.

21. A method for providing access management through use of a distributed network of server machines, said method comprising the acts of:

(a) receiving, at first server machine of the plurality of server machines, an access request to access secure items from a user of a first client machine;

(b) authenticating the user of the client machine;

(c) authenticating the first client machine;

(d) retrieving access privileges associated with the user;

(e) determining whether the user is permitted to gain access to secure items via the first server machine based on the access privileges when said authenticating (b) and (c) are successful;

(f) permitting the user to gain access to secure items via the first server machine when said determining (e) determines that the user is permitted to gain access to secure items via the first server machine; and

(g) preventing the user to gain access to secure items via the first server machine when said determining (e) determines that the user is not permitted to gain access to secure items via the first server machine.

22. A method as recited in claim 21, wherein said method comprises the acts of:

(h) preventing the user from gaining access to secure items via any of the server machines other than the first server machine when said determining (e) determines that the user is permitted to gain access to secure items via the first server machine.

23. A method as recited in claim 21,

wherein said determining (e) further determines whether the user is permitted to gain access to secure items via the first client machine, and

wherein said permitting (f) operates to permit the user to gain access to secure items via the first client machine and the first server machine when said determining (e) determines that the user is permitted to gain access to secure items via both the first client machine and the first server machine.

24. A method as recited in claim 23, wherein said method comprises the acts of:

(h) preventing the user from gaining access to secure items via any of the server machines other than the first server machine when said determining (e) determines that the user is permitted to gain access to secure items via the first server machine.

25. A method as recited in claim 24, wherein said preventing (h) of the user to gain access to secure items via any of the other server machines comprises reconfiguring at least any of the other server machines that previously permitted the user to gain access to secure items therethrough.

26. A method as recited in claim 25, wherein said permitting (f) of the user to gain access to secure items via the first server machine comprises

reconfiguring the first server machine to permit access by the user to secured items via the first server machine.

27. A method as recited in claim 21, wherein said permitting (f) of the user to gain access to secure items via the first server machine comprises reconfiguring the first server machine to permit access by the user to secured items via the first server machine.

28. A method as recited in claim 21, wherein each of the secure items is a secured file, the secured file having a format that comprises a header including security information as to who and how the secure item can be accessed; an encrypted data portion including data of the secure file encrypted with a file key according to a predetermined cipher scheme, and wherein the header is attached to the encrypted data portion to generate the secured file.

29. A method as recited in claim 28, wherein the security information in the header of the secured file facilitates the restricted access to the secured file.

30. A method as recited in claim 28, wherein the security information is encrypted with a user key associated with a user.

31. A method as recited in claim 28, wherein the security information includes the file key and access rules to the restricted access to the secured file.

32. A method as recited in claim 28, wherein the file key is retrieved to decrypt the encrypted data portion in the secured file when access privilege of the user is within access permissions by the access rules.

33. A method as recited in claim 31, wherein the access rules are expressed in a markup language.

34. A computer readable medium including at least computer program code for providing access management to secured content through use of a plurality of server machines associated with different locations, said computer readable medium comprising:

computer program code for receiving, at a first server machine of the plurality of server machines, an access request to access secured items from a user of a first client machine at a first location;

computer program code for authenticating the user of the first client machine at the first location;

computer program code for authenticating the first client machine;

computer program code for determining whether the user is permitted to gain access to secured items via the first location when said computer program code for authenticating the first client machine and the user are successful;

computer program code for permitting the user to gain access to secured items via the first server machine when said computer program code for determining determines that the user is permitted to gain access to secured items from the first location; and

computer program code for preventing the user to gain access to secured items via the first server machine when said computer program code for determining determines that the user is not permitted to gain access to secured items from the first location.

35. A computer readable medium including at least computer program code for providing access management through use of a distributed network of server machines, said computer readable medium comprises:

computer program code for receiving, at first server machine of the plurality of server machines, an access request to access secure items from a user of a first client machine;

computer program code for authenticating the user of the client machine;

computer program code for authenticating the first client machine;

computer program code for retrieving access privileges associated with the user;

computer program code for determining whether the user is permitted to gain access to secure items via the first server machine based on the access privileges when said computer program code for authenticating the first client machine and the user are successful;

computer program code for permitting the user to gain access to secure items via the first server machine when said computer program code for determining determines that the user is permitted to gain access to secure items via the first server machine; and

computer program code for preventing the user to gain access to secure items via the first server machine when said computer program code for determining determines that the user is not permitted to gain access to secure items via the first server machine.

36. An access control system that restricts access to secured items, said system comprising:

a central server having a server module that provides overall access control; and

a plurality of local servers, each of said servers including a local module that provides local access control,

wherein the access control, performed by said central server or said local servers, operates to permit or deny access requests to secured items by requestors, and

wherein a given requestor is only able to access secured items using only a single one of said local servers or the central server such that the given requestor can only access secured items through at most one of said local servers at a time even though the given requestor is permitted to access secure items through more than one of said local servers.

37. An access control system as recited in claim 36, wherein said access control system couples to an enterprise network to restrict access to secured files stored therein.

38. An access control system as recited in claim 37, wherein the access requests are at least primarily processed in a distributed manner by said local servers.

39. An access control system as recited in claim 38, wherein when the access requests are processed said local servers, the requestors gain access to the secured files without having to access said central server.

40. An access control system as recited in claim 37, wherein the local module can be a copy of the server module so any of the local modules can operate independent of said central server and other of said local servers.

41. An access control system as recited in claim 37, wherein the local module can be a subset of the server module.

42. An access control system as recited in claim 37, wherein access permissions for said local servers can be dynamically configured to pass a requestor from one of said local servers to another of said local servers, thereby enabling access control to be performed by the another of said local servers such as when the location of the requestor changes.

43. An access control system as recited in claim 37, wherein the secured files are secured files.

44. An access control system as recited in claim 37, wherein the secured files are secured by encryption.